Appropriate Filtering for Education settings

May 2024

Filtering Provider Checklist Reponses

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.*"

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Wave 9 Managed Services Limited
Address	1 Hargreaves Court, Staffordshire Technology Park, Stafford ST18 0WN
Contact details	Lee Neely lee.neely@wave9.co.uk
Filtering System	WaveConnect – Managed Educated Internet Service incorporating Sophos XGS and Lightspeed Systems
Date of assessment	8.9.24

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	🟩
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	🟨

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
● Are IWF members	🟩	Wave 9, Sophos and Lightspeed are IWF Members
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list), including frequency of URL list update	🟩	Yes, WaveConnect actively implements the IWF URL list
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Yes, WaveConnect actively integrates the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.
● Confirm that filters for illegal content cannot be disabled by anyone at the school (including any system administrator).	🟩 Sophos	All categories associated with illegal content are blocked at System Level and cannot be disabled at the school.
	🟩 Lightspeed	All websites categorised as illegal in Lightspeed's extensive, constantly updated URL database are placed in sealed categories that cannot be allowed by any IT admin or member of staff in a school or organisation.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.	🟩 Sophos	The category "Intolerance and Hate" which would cover content that promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex is blocked by default.
		🟩	When a user attempts to search for anything, a list of keywords is referenced. If the search includes

			any discriminatory or offensive words on the list, access will be blocked. Our importable flagged keyword list contains hundreds of entries, and admins can customise the list with their own keywords that best match their communities.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	Sophos	The “Controlled substances category” along with “Legal highs” and “Marijuana” which cover content that displays or promotes the illegal manufacture, trade or use of drugs or substances are blocked by default
		Lightspeed	We have specific categories for blocking access to drugs and alcohol.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	Sophos	Our standard deployment for Education would block the category “Intolerance and Hate” It would also block the category “Criminal Activities” which would include the “Counter Terrorism Internet Referral Unit” list. This would cover sites that promote terrorism and terrorist ideologies, violence, or intolerance.
		Lightspeed	Our violence extremism category contains all of the latest URLs from the Home Office that promote terrorism, terrorist ideologies, violence or intolerance—as well as URLs added by the worldwide education community.
Gambling	Enables gambling	Sophos	Wave 9 standard deployments would block any website which falls under the Gambling category, for all user-types, be they staff or student. If no user-based-filtering is performed or possible, the Gambling category is blocked by

			the unauthenticated web policy.
		Lightspeed	Lightspeed Filter’s gambling category blocks all websites related to gambling, casinos, betting, lottery and sweepstakes.
Hate speech	Content that expresses hate or encourages violence towards a person or group based on something such as race, religion, sex, or sexual orientation	Sophos	WaveConnect provides an “Intolerance and Hate” category to enable blocking of sites that foster racial supremacy or vilify/discriminate against groups or individuals. This is blocked by default
		Lightspeed	Lightspeed blocks these sites using a combination of categories including Violence, Extremism, Mature
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	Sophos	Wave 9 provides an “Anonymizers”, “Hacking, Phishing and Fraud”, “Spam URLs” and “Spyware and Malware” categories. Wave 9 block these categories. In addition, all unencrypted content is scanned for malware. A cloud-delivered sandbox analyses any downloaded active content and blocks malware. This category is included in our default Safeguarding list.
		Lightspeed	Malware and other malicious content is blocked before it reaches the network. Our database categorises sites with demonstrated or potential security risks into several security categories, and for extra safety, all unknown URLs can be blocked.
Pornography	displays sexual acts or explicit images	Sophos	Wave 9 includes “Sexually Explicit”, “Nudity” and “Extreme” categories. Wave 9 block these categories. Also, Wave 9 provides “Safe-Search” enforcement on the major search engines.
		Lightspeed	all pornographic material in the porn category is

			blocked. In addition, potentially illegal pornographic material is locked as well as a second category porn.illicit containing potentially illegal pornographic material. This is a sealed category and cannot be unblocked.
Piracy and copyright theft	includes illegal provision of copyrighted material	Sophos	Wave 9 standard deployments would block sites supporting, enabling, or engaging in sharing of content that is protected intellectual property and websites that provide, distribute or sell school essays, projects, or diplomas. The option is also available to add a “Creative Commons” license that only shows images published under Creative Commons licensing laws
		Lightspeed	Our category forums.p2p blocks access to all peer-to-peer and file-sharing sites that would enable plagiarism or sharing copyrighted material
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	Sophos	Wave 9 standard deployments would block Sites promoting suicide and self-harm. These categories are included in our default Safeguarding list.
		Lightspeed	To prevent any students from looking at websites that promote or display self-harm, again the blocked-search key words is referenced; and a number of different categories can be controlled such as forums and adult. Our safeguarding solution Lightspeed Alert™ built into the uses advanced AI and a 24/7 safety specialist team to notify administrators instantly when a student types anything relating to self-harm online. Alert works across all productivity and education apps, files, chat including Microsoft Teams and Google Workspace and provides

			schools with a timeline of the event including screenshots and activity logs.
Violence	Displays or promotes the use of physical force intended to hurt or kill	Sophos	Wave 9 provides “Extreme” and “Criminal Activity” categories. Wave 9 block these categories to block sites displaying or promoting the use of physical force intended to hurt or kill. These categories are included in our default Safeguarding list.
		Lightspeed	Our violence category contains all sites that promote the use of physical force intended to harm or kill. Lightspeed Alert also notifies schools and admins when students type anything related to violence

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Sophos:
The system currently provides 91 different URL categories. For the full list see: https://www.sophos.com/threat-center/reassessment-request/utm.aspx.

Sophos Labs enables us to dynamically update our web categories by providing a URL categorisation services that integrate Sophos URL data with that of multiple third-party suppliers, including IWF and CTIRU, to provide a market-leading database.

We classify sites at the IP, domain, sub-domain level and path URL data is constantly reviewed, and unclassified websites are classified on an hourly basis.

Lightspeed:
Lightspeed Systems uses our online database that leverages AI, machine learning, and the infinite cloud for the most accurate and comprehensive categorisation of the Web. Schools have the ability to restrict access to certain categories or to unknown URLs

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained.

Sophos:
Data retention is at the discretion of the customer and beyond any policy requirements (E.g. the GDPR) policy is only limited by the storage capacity of the schools filtering appliance and any archive logs they may choose to keep. The school is the data controller and so should determine their data retention requirements in line with their policy.

Lightspeed:
We retain data for as long as necessary to fulfil the purposes for which it was collected for. Following termination or deactivation of a School account, Lightspeed Systems may retain profile information and content for a commercially reasonable time for backup, archival, or audit purposes, but all Student Data associated with the School will be deleted in accordance with Lightspeed Systems Data Deletion policy, or in accordance with active DPA, DSA or SLA. We may maintain anonymised or aggregated data, including usage data, for analytics purposes

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Sophos:
Our database is in use on over 300 million devices worldwide. This provides a uniquely large user community that reports category misclassification requests directly to the service.

Currently, fewer than 50 of these requests are made per day. This lack of customer complaint demonstrates clearly that the category database is of the highest standard. Furthermore, most of the reported URLs are not reclassified as review ordinarily determines the original classification is correct.

We also provide tools that enable customers to create custom categories that over-ride current URL database classifications and end users to request page reclassification, by the system administrator, directly from the block page or via the Wave 9 Helpdesk.

Lightspeed:
Customers are able to customise the filter to meet their local needs including allowing or blocking categorise, domains, URLs and IPs. Additionally, customers are able to configure the filter to allow normally blocked site for a period of time. Finally, as an education only based company our database is tuned for education by education via our share option where customers can share category changes with us.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
● Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff	Sophos	Wave 9 can apply policy rules based on group information, usually the schools Active Directory. If the school includes objects related to age, year group, role then policies can be created that open certain categories of websites once a certain age has been reached (e.g. the "Sex Education" category). Wave 9 also logs all user group activity separately for reporting. Reports can be generated for a specific event in a specific user group. All alerts

		can be sent using a syslog into a security incident and event management system (SIEM)
	Lightspeed	Lightspeed Filter has been designed specifically for education. It can be fully customised to perfectly match your organisational structure-tailoring policies based for different year groups, ability, location or for members of staff.
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services, DNS over HTTPS and ECH.	Sophos	Wave 9 provides the “Anonymizers’ category in our web filter. Wave 9 blocks this category . Whilst we also provide a ‘block filter avoidance app’ application rule. Both policies would block users from being able to circumvent their filtering
	Lightspeed	Lightspeed’s patent-pending Smart Agents filter any device, any app, any browser; and provide easy SSL decryption without proxies, PACs, or certificate hassles. Our extensive database of URL’s is constantly being updated with the latest VPN’s and filter bypassing tools and keeping them blocked.
● Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes	Sophos	Our service is Co-administered with the establishment allowing nominated members of staff control of the filter policies or assistance from our qualified helpdesk staff. Temporary “unblocking” can be achieved “ad-hoc” at the discretion of the school by an authorised member of staff with limited delegated admin rights
	Lightspeed	Tiered administration across our products allows different levels of control to be permitted to different schools and users. Designated staff can add and

		edit keyword lists and create local allow and block lists. YouTube access can be managed by category, channel, and video. Using Lightspeed Classroom Management™, teachers can allow or block URLs to expand or constrict access with oversight.
● Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter, including GenAI content such as ChatGPT.	Sophos	The Sophos XG includes a content scanning feature, whereby URLs and web pages are dynamically analysed for specific keywords or phrases. Customers can upload multiple keyword lists to support different languages and provide better granularity. Any pages matching words or phrases contained within the keyword lists can be blocked and/or logged. In addition, Administrators/Safeguarding officers can review the blocked keywords using the onboard log viewer and determine the context.
	Lightspeed	Lightspeed Filter utilises a database system that dynamically scans page content to ensure that the page is correctly categorised.
● Deployment – filtering systems can be deployed in a variety (and combination) of ways (eg on device, network level, cloud, DNS). Providers should describe how their systems are deployed alongside any required configurations	Sophos	The Sophos Firewall solution is available as a physical appliance, virtual appliance or as an image on AWS (bring your own licence or pay as you go) or on Azure. Network traffic is then passed through the appliance as required for Firewall or web filtering. Also available as an device based agent utilising Central Intercept X Advanced client
	Lightspeed	Lightspeed is deployed in a variety of ways, including device based Agents, onsite network agent on a local VM (usually for

		unmanaged devices) or DNS filtering based in the cloud.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	Sophos	Our Service Level Agreement (SLA) outlines the default polices applied with our service. Any changes to these are agreed with the establishment dependent on school context and assessment of risk. Our rationale is published in our “Security, Safeguarding and Prevent” documentation for WaveConnect Education service
	Lightspeed	The adaptive AI database of Lightspeed Systems leverages AI, machine learning and the infinite cloud for the most accurate and comprehensive categorisation of the Web. This means you save time not having to re-categorise, and you can count on students staying safe without over blocking.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	Sophos	Wave 9 can provide a management console that enables the customer to manage multiple sites in one console. Central policy can be configured and pushed out to multiple sites. Whilst reporting and alerting can all be managed centrally
	Lightspeed	Lightspeed Filter allows tiered levels of control based on user’s roles in the organisation, as well as centralised policies that work across entire schools, local authorities or trusts
• Identification - the filtering system should have the ability to identify users	Sophos	Our services as a multitude of different ways of identifying users, both transparent (e.g. NTLM or SAML) and non-transparent (e.g. Captive Portal).

		Typically, we use “Active Directory” single sign-on to identify users
	Lightspeed	Lightspeed Filter can integrate with authorisation sources to gather user credentials, be configured for a captive portal or use local accounts. Lightspeed identifies users through a range of different methods including a web portal, agent (application) identification, and RADIUS integration.
● Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps and any configuration or component requirements to achieve this	Sophos	Our service can be deployed in transparent mode, adding this to the “Guest” Wi-Fi provided by the establishment can be easily achieved. Users need to be identified by the use of the “Captive Portal”, users must authenticate first. If HTTPS decryption is deployed, the block page can display the security certificate that needs to be deployed to the mobile device(s) and instructions on how to install the security certificate on the mobile device so alerts are no longer seen. However, deploying HTTPS to many APPS may have an adverse effect as they employ “certificate pinning” and may not allow decryption. In this case, an HTTPS decryption exception will need to be added manually with the support of our Helpdesk staff, which is included within the WaveConnect Education support SLA. Please note that this does not cover 3G/4G cellular data services or devices not connected to the establishment's internal

		network (e.g. home broadband)
	Lightspeed	All traffic that passes through a school or college network can be intercepted, including content via mobile and app technologies. If inappropriate apps are the issue, Lightspeed Mobile Device Management™, utilises app management to control device apps and restrictions.
● Multiple language support – the ability for the system to manage relevant languages	Sophos	Wave 9 supports multiple block pages to support multiple languages and custom block pages where multiple languages are required on the same page.
	Lightspeed	Our world categories contain websites from multiple countries that can be filtered accordingly. Flagged keywords can be added in any language to flag suspicious or concerning user activity. Further, we can enforce Google safe search, which has Google's own rules in multiple languages
● Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school	Sophos	We have three options addressing remote working that schools can opt for depending on the extent to which this applies to a particular establishment. At a based level all our services include remote access VPN as standard and when enforced by device management all traffic is router via the school based web filter. A second option is to enforce a filtering policy using the Sophos Central Endpoint protection

		client. This includes web control, which has specific policies for remote devices. These policies can be managed via Sophos Central (Cloud management platform) and any violations can be reported on. There are over 48 categories that can be configured, as well as file type blocking. This includes sites that are on the IWF and Counter Terrorism Referral Unit block lists. For schools where there are large numbers of student devices being used at home and in school, we can deliver the option of filtering and monitoring using an agent based solution based on Lightspeed.
	Lightspeed	Lightspeed Filter uses patented Smart Agents that sit on every device to give schools the same level of filtering on any device and any OS remotely. Schools can also enable “after school rules” and time or location-based policies to these devices to ease restrictions accordingly
● Reporting mechanism – the ability to report inappropriate content for access or blocking	Sophos	There is the ability to report inappropriate content via a web portal or by request to our help desk.
	Lightspeed	We provide an extensive list of reporting and options to create customised and easily shareable reports.
● Reports – the system offers clear historical information on the websites users have accessed or attempted to access	Sophos	A range of standard and customisable reports can be viewed or automated by email that shows user activity.
	Lightspeed	Admins have immediate access to pre-installed web activity reports that may be customised by date range, school, and group.

- Safe Search – the ability to enforce 'safe search' when using search engines	Sophos	SafeSearch is enforced by both the Authenticated and Unauthenticated web policies for the search engines google.com/uk, bing.com and yahoo.com/uk. All other search engines are blocked, thus providing only Safe Search entry points to those search engines where Safe Search enforcement is possible.
	Lightspeed	We allow schools to force Safe Search for the entire school or individual groups

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum".*[1]

Please note below opportunities to support schools (and other settings) in this regard

Wave 9 is 100% focussed on the provision of safe, secure Internet connectivity and infrastructure to Education. Our leadership team have been involved in the provision of internet and filtering services to education since the late 1990's.
Our services are designed and delivered in a way that ensures our school customers benefit from a service that exceeds the requirements set out in Annex C of KCSIE

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Provider Self-Certification Declaration

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Lee Neely
Position	Director
Date	12 September 2024
Signature	